AIR WAR COLLEGE

AIR UNIVERSITY

EVOLVING INTELLIGENCE, SURVEILLANCE & RECONNAISSANCE (ISR)

FOR

AIR FORCE CYBER DEFENSE

by

Frederick E. Bush III, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Col Jill E. Singleton, USAF

14 February 2013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
14 FEB 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Evolving Intelligence, Surveillance & Reconnaissance (ISR)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University,Air War College,Maxwell AFB,AL,36112**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The United States Air Force is at a critical time in its history. Since the end of World War II, the Air Force has enjoyed qualitative technology superiority over its adversaries. With the development of the cyber age, this technology advantage gained by the Air Force has been continuously under assault. The rapid advance of cyberspace operations is driving an imperative to evolve Intelligence, Surveillance and Reconnaissance (ISR) for the Air Force. Within this context, ISR can be the impetus for proactive defense within the cyberspace domain. The existing Air Force ISR capability for support to defensive cyberspace operations has to operate in an environment of global adversaries. The effectiveness of Air Force defensive cyber strategy will depend on long range trend analysis of adversary capabilities and intent. An evolution of ISR for cyber defense can improve protection of key Air Force command and control functions, as well as best preserve the Air Force?s qualitative technology advantage against adversary network reconnaissance and attack activities. This paper provides several recommendations to advance ISR for cyber defense. The Air Force should develop a robust ISR Processing, Exploitation and Dissemination (PED) capability devoted to cyberspace. Additionally, the Air Force should conduct an in-depth study to determine resources required for the National Air and Space Intelligence Center to grow capacity for more robust analysis of adversary cyber capabilities. Next, a stronger cyber defensive strategy, enabled by ISR, will require additional intelligence resources or realignment of existing resources in the Air Force ISR Agency and 24th Air Force. ISR capabilities will be the catalyst for cyber defense of critical assets to more fully protect commanders? air, space and cyber operations.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**24**	

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Frederick E. Bush III is a US Air Force intelligence officer assigned to the Air War College, Air University, Maxwell AFB, AL. He graduated from the University of Alabama in 1992 with a Bachelor of Arts degree in History, and Troy University in 2001 with a Masters of Public Administration. He has served in a variety of intelligence and cyber assignments ranging from squadron to joint level, both in-garrison and deployed. He has commanded an Imagery Analysis Squadron and a Network Warfare Squadron. Most recently, he was the deputy commander of the 26th Network Operations Group.

Abstract

The United States Air Force is at a critical time in its history. Since the end of World War II, the Air Force has enjoyed qualitative technology superiority over its adversaries. With the development of the cyber age, this technology advantage gained by the Air Force has been continuously under assault. The rapid advance of cyberspace operations is driving an imperative to evolve Intelligence, Surveillance and Reconnaissance (ISR) for the Air Force.

Within this context, ISR can be the impetus for proactive defense within the cyberspace domain. The existing Air Force ISR capability for support to defensive cyberspace operations has to operate in an environment of global adversaries. The effectiveness of Air Force defensive cyber strategy will depend on long range trend analysis of adversary capabilities and intent. An evolution of ISR for cyber defense can improve protection of key Air Force command and control functions, as well as best preserve the Air Force's qualitative technology advantage against adversary network reconnaissance and attack activities.

This paper provides several recommendations to advance ISR for cyber defense. The Air Force should develop a robust ISR Processing, Exploitation and Dissemination (PED) capability devoted to cyberspace. Additionally, the Air Force should conduct an in-depth study to determine resources required for the National Air and Space Intelligence Center to grow capacity for more robust analysis of adversary cyber capabilities. Next, a stronger cyber defensive strategy, enabled by ISR, will require additional intelligence resources or realignment of existing resources in the Air Force ISR Agency and 24th Air Force. ISR capabilities will be the catalyst for cyber defense of critical assets to more fully protect commanders' air, space and cyber operations.

Introduction

A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11. Such a destructive cyber terrorist attack could paralyze the nation.[1]

-Secretary of Defense Leon Panetta

This statement from the Secretary of Defense underscores the importance of strong cyber defenses for the nation. Intelligence plays a vital role in determining optimal actions and strategies to defeat adversary cyber operations against the United States. Current Air Force defensive cyber operations depend upon already established centers of excellence for ISR that are designed to support traditional airpower operations. Cyber defense resources belong predominately to the Air Force Intelligence Surveillance and Reconnaissance Agency (AFISRA) and other Joint and DOD Agencies. This structure evolved over time to support cyber activities not linked to the integrated Air Force Network (AFNET). As the AFNET becomes more mature, Air Force ISR activities, capabilities and analysis for defensive cyber operations should expand into a comprehensive cyber defense operations strategy to best stop and defeat the adversary.

Background

In the cyberspace domain, the art of defense is absolutely critical to ensuring freedom of operations. Starting at the nation state level, the defense of cyber networks is very important; intelligence plays a key role in this defense. According to Jeffrey Carr, "the core responsibility of intelligence as a discipline is to provide state leadership with insight into what the emerging threats are before they manifest into an attack on the state."[2] This view of the role of predictive intelligence should be applied to Air Force cyber defense, to proactively engage in defensive operations and strategies against threats to the Air Force's networks.

Within the realm of intelligence at the national-level and within the Department of Defense, "the primary function of joint intelligence is to provide information and assessments to

facilitate accomplishment of the mission."[3] This responsibility for intelligence is inherent within the established military domains of air, space, maritime, and ground operations. This ranges the spectrum of intelligence from near-real-time intelligence operations to long range trend analysis of adversary threats, intentions and capabilities. Cyber operations have no less of a requirement for intelligence to accomplish the Air Force mission; this requirement is even more important for mission activities associated with defense of critical networks.

It is the inherent responsibility of a military service to defend its critical mission networks within the cyberspace domain. In the case of the United States Air Force, its mission is to "Fly, fight and win in Air, Space & Cyberspace."[4] More specifically, it is the role of the Air Force to defend its critical operations within cyber networks to ensure total mission assurance. Just as ISR is a key component of effective mission planning for Defensive Counter Air execution in combat air operations, ISR within cyberspace is critical for effective cyber defense operations with contributions ranging from predicting adversary intentions and capabilities to full spectrum cyber battle damage assessment.

Historically, Air Force network defense tended to be passive and reactive in nature. It depended on intelligence of adversary activity to stop short term threats. Defensive actions were prompted by adversary activity which penetrated Air Force networks. Intelligence was limited to mitigating damage from exfiltration of data weeks or months after the event. There was little capability for strategic defensive actions, beyond signature detection, to proactively stop or degrade an adversary's capability of accessing or penetrating Air Force networks. Additionally, most defensive cyber activities have tended to focus on protection of the NIPRNET, leaving only passive security measures for the most critical of Air Force mission systems. The Air Force NIPRNET is defined as a computer network for unclassified, but sensitive information

supporting the Department of Defense.[5] The challenge of focused defense was well articulated by Brigadier General Kevin Wooton, the Director of Communications and Information at Air Force Space Command, when he noted that "historically we defended the base library to the same level as a Wing Commander's computer."[6] This network defense methodology was not based on any specific cyber intelligence to drive operations, but rather a belief that everything can and should be defended to the same level within the cyber domain. General Wooton, a career intelligence officer and former commander of the 67th Network Warfare Wing, is uniquely qualified to comment on the role of intelligence within the cyberspace domain.

As the need for a deliberate cyber defense strategy emerges within the Air Force, the role of ISR in driving defensive cyber operations specific to the Air Force is becoming more pronounced. The Director of National Intelligence James Clapper noted, "we foresee a cyber-environment in which emerging technologies are developed and implemented before security responses can be put in place."[7] In this context, the need for defensive cyber strategy keyed by intelligence is critical to blunt ongoing adversary activities targeting Air Force networks.

The following unclassified and open-source examples of adversary cyber activities with notional implications for the Air Force are included for operational perspective to demonstrate how cyber intelligence can play an increased role. Cyber defense threats range from sophisticated nation state and military actors down to the hacktivist or extremist groups not affiliated with any country. These adversary cyber threats operate against the spectrum of United States government, military, and defense industry capabilities. Adversaries are already targeting the Air Force's core capabilities. An evolution in ISR to radically enhance predictive analysis support to cyber defense can stop adversaries more effectively.

Adversary cyber collection and attack capabilities focused on United States military networks continue to evolve at a rapid rate. The People's Republic of China (PRC) gets the most attention for targeting United States cyber networks. According to Carr, "(since 2001)… most of the PRC's focus has been on cyber espionage activities in accordance with its military strategy to focus on mitigating the technological superiority of the US military."[8] According to Stokes and Hsiao, Chinese targeting is "characterized by methods of encrypting exfiltrated data, attempts to gain control and access to U.S. computer systems rely in large part upon socially engineered email messages that may seem authentic targeting organizations and individuals of interest."[9] Furthermore, the impact of China's cyber activities was noted in the 2012 US-China Economic and Security Review Commission Report to Congress stating, "Chinese penetrations of defense systems threaten the U.S. military's readiness and ability to operate."[10] This active targeting surely extends into the Air Force, as shown in a 2009 article in the Wall Street Journal which implied the Chinese exfiltrated data on the F-35 Joint Strike Fighter (JSF), including "several terabytes of data related to the design of electronic systems."[11]

China is far from alone; Russia, Iran, North Korea, and non-state actors are focusing on improving their cyber expertise. Russian cyber capabilities are very sophisticated, according to open source information. The Russian military and government security services have a robust capability, as demonstrated in the last decade by very effective offensive cyber capabilities during crises with Estonia, Georgia, and South Ossetia.[12] According to Clarke, "the Russians are definitely better (than China), almost as good as we are (the United States)."[13] Furthermore, the Iranian Revolutionary Guard Corps (IRGC) has a cyber warfare division with the capability to employ "…computer viruses and worms, cyber data collection, exploitation, computer and network reconnaissance."[14] North Korea also possessed a cyber threat, according to unclassified

press and media sources. For example, numerous press reports speculated that North Korea executed distributed denial of service attacks aimed at White House and other government web sites.[15] There are also threats in the realm of non-state cyber actors, ranging from Jihadist associated cyber actors with anti-US sentiments, all the way to political hacktivists.[16] As potential bad actors emerge on the Global Information Grid, Air Force cyber defense operations must be better postured through effective ISR to best provide full cyber mission assurance.

Current Air Force Cyber Defense Posture and ISR

Understanding of the current Air Force cyber defense posture and the ISR contribution to it is useful now that the cyber operational threat is established. Elements of the AFISRA are charged with providing ISR support to defensive cyber operations. This analysis comes directly from the 35th Intelligence Squadron (35 IS), part of the larger 659th ISR Group (659 ISRG). This squadron provides tailored support for the cyber defense mission, but is under-resourced from a personnel perspective for the mission it is tasked to perform. Unique to this capability is the small National-Tactical-Integration (NTI) capability for cyber intelligence within the 35 IS. This activity is small scale and effective given current resources, but has untapped potential to provide broader, operationally effective ISR data for cyber defense. The operational focus tends to be on near-real-time operations, with little capability/capacity for adversary trend analysis for longer range threats. Additionally, the mission to perform analysis of the emerging threat from adversary malware is tasked to the National Air and Space Intelligence Center (NASIC) Command Control Communications and Computers / Information Operations (C4/IO) Squadron. According to Colonel Carl Brenner, the Commander of the NASIC Air & Cyber Analysis Group, the C4/IO Squadron has little capacity to perform long-range trend analysis of adversary cyber threats at the level of NASIC's well-established air and space intelligence support.[17] These Air

Force cyber intelligence units provide reporting which can be combined with reporting from joint, sister-service and national agencies.

Historically, Air Force network defense was based on a distributed architecture of intrusion detection systems known as ASIM (Automated Security Incident Management). This system provided evidence of adversary entrance and exit from the network, but was signature based and provided no capability for automatic blocking, tracking, forensics, or pattern of activity development. These systems were deployed at the base level, and provided a near-real-time but conceptually limited view of the cyber battlespace. Additionally, as adversary cyber tactics improved, ASIM provided ever more limited data for long-range trend analysis. The ASIM architecture contributed to the "defend everything" cyber strategy previously described, and had more limited intelligence interaction than might at first appear. This system was retired in 2011, and replaced with a series of more robust cyber defense systems to implement the strategy known as "Defense-In-Depth." According to a National Security Agency paper on Defense-in-Depth, the strategy works to "deploy protection mechanisms at multiple locations to resist all classes of attacks."[18] The Air Force's Defense-In-Depth strategy, as indicated by Lieutenant Colonel Joe Zell, Commander of the 33rd Network Warfare Squadron (33 NWS), employs a variety of cyber defense sensors ranging from the Air Force Gateway level down to the individual host computer desk top level.[19] Each of these network defense sensors and applications has a variety of potential Cyber ISR functionalities.

Air Force cyberspace operations lack a robust capability for Processing, Exploitation and Dissemination (PED) for intelligence data to support cyber defense. The architecture described above does not enable intelligence support for active cyber defense in a manner like that of other more mature capabilities. For comparison, the Air Force Distributed Common Ground System

(AFDCGS) provides a mature PED capability for data from imagery and signals intelligence sensors. The following figure shows the current structure of the Air Force DCGS, which provides world-class ISR for the established domains of military operations. With this as a well-established operational guide, something comparable for cyberspace should be considered for development.

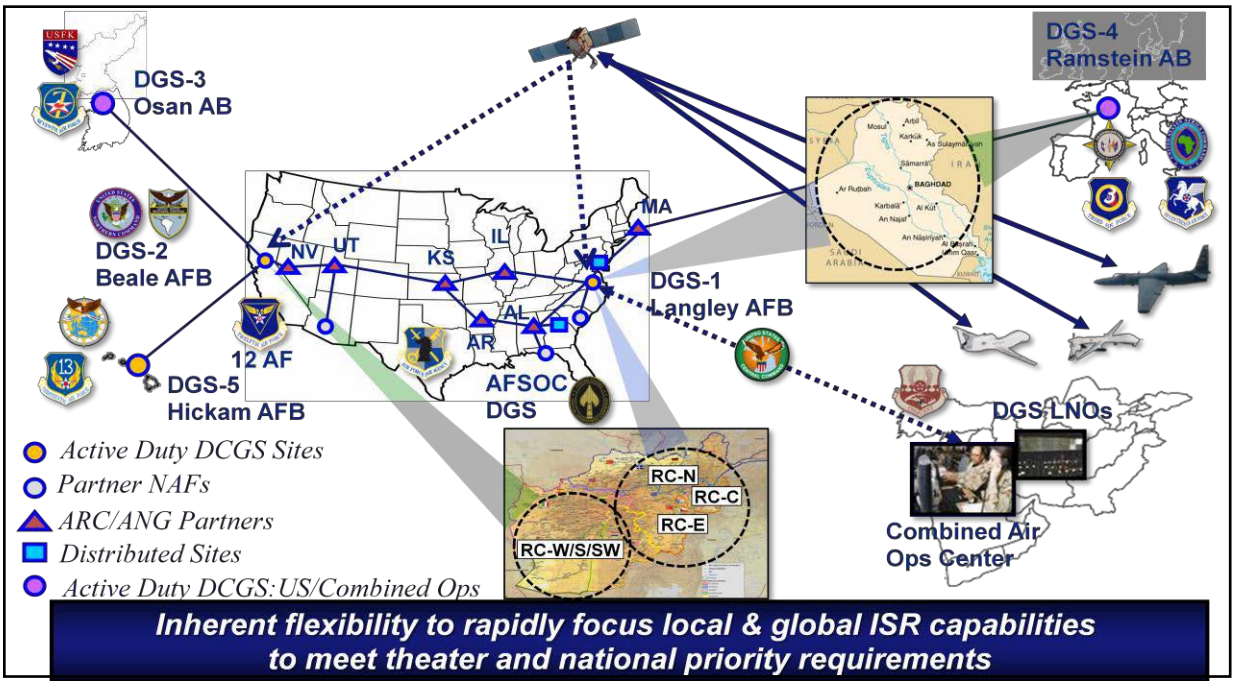

Figure 1- Air Force DCGS Operation[20]

The type of robust PED structure described for cyberspace could provide critical intelligence for defense against continuous adversary cyber attacks. For instance, DoD networks, Air Force core capabilities and future programs are routine targets for adversary network attacks, according to numerous open-source media examples. The adversary targeting aims at many of the Air Force core missions to include nuclear deterrence operations, air superiority, space superiority, cyberspace superiority, global precision attack, rapid global mobility, special operations, global integrated intelligence, surveillance and reconnaissance, and

command and control.[21] These operational programs are assigned to MAJCOM commanders as Core Functional Lead Integrators (CFLIs). The main Air Force operational program targets range the spectrum from bombers, air mobility, fighters, Intercontinental Ballistic Missiles (ICBM), to space and cyber capabilities. These all represent operational data types routinely targeted by the adversary.

As a corollary to cyber defense operations, the Air Force Telecommunications and Assessment Program (TMAP) notes in Air Force Instruction (AFI) 10-712 that "adversaries can easily monitor (unclassified) systems to gather information regarding military capabilities, limitations, intentions, and activities."[22] Increased adversary targeting of these CFLI identified capabilities and programs has strong potential to erode the Air Force's current qualitative advantage over global adversaries. Given the nature of defense within the cyberspace domain, there will never be enough cyber defense sensors to effectively defend all critical Air Force networks. Robust ISR for Air Force Cyber Defense should be used in the future to effectively focus defensive strategies to blunt adversary activities. Robust and predictive ISR, when combined with highly effective Air Force cyber defense capabilities, has great potential to vector cyber defenses to best defend these critical Air Force capabilities. This critical role of ISR for cyber defense is supported by Lieutenant Colonel Mike Ragland, the commander of the 68th Network Warfare Squadron (68 NWS) at Joint Base San Antonio-Lackland Air Force Base.[23]

Intelligence Processes

Air Force intelligence as a discipline has a very well defined intelligence cycle, which provides a framework of how data is gathered and analyzed to produce an operational intelligence product. The main parts of the Air Force intelligence cycle include planning and

direction, collection, processing and exploitation, analysis and production, and dissemination. These five steps are well developed for ISR support to the air and space domains of warfare.

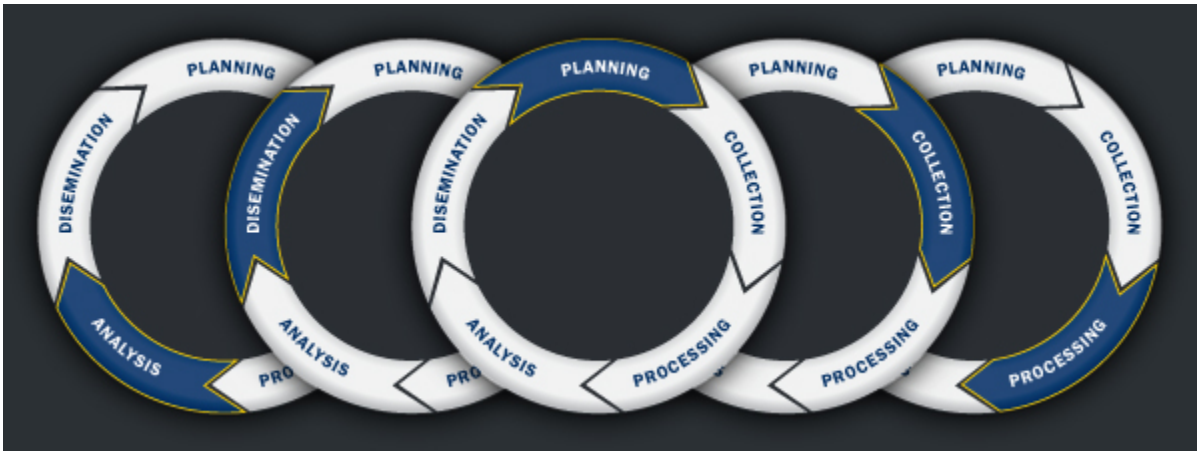

Figure 2 - Intelligence Cycle[24]

Specified support for operations within the cyberspace domain for the intelligence cycle is not yet well developed to be the trigger for large-scale, cyber defense strategies in the Air Force, according to Lieutenant Colonel Scott Vickery, commander of the 26th Operations Support Squadron (26 OSS) located at Joint Base San Antonio-Lackland Air Force Base.[25] Currently limited Air Force and Joint cyber intelligence reporting "makes cyber defense very reactive in nature and heavily dependent on national agency reporting which may not be specifically tailored for Air Force requirements."[26] At its best, Vickery contends cyber intelligence support "is right here, right now and of a very time sensitive nature only."[27] After cyber intelligence reporting is approximately seventy two hours old, the reporting on probable adversary activity or intentions tends to lose much operational value. Furthermore, there is very little within Air Force ISR to support long-range cyber trend analysis of adversary capabilities, trends and intentions. Nor is ISR focused to help protect Air Force core technologies or capabilities. As of today, there is no document for defensive cyber operations which is

equivalent to the foundational "Threat to Air Operations" series which helped guide ISR support to air or space weapon systems and tactics to counter specified adversary nations around the globe.[28]

Regarding the nature of defensive operations within the cyber domain, there are some unique attributes for this area of warfare. In traditional combat operations, there is an inherent advantage to the defender when conducting operations. The reverse is true for this rule within cyber warfare; the attacker has a built in advantage over those who defend.[29] Furthermore, Major General Brett T. Williams, the current USCYBERCOM Director of Operations noted a unique operational characteristic of cyberspace where, "defense as the main effort is the key difference between cyber and the terrestrial domains."[30] Within cyber defense, the traditional Air Force model called for defending the entire attack surface of Air Force associated cyber networks to the same level. This approach provided ample room for advanced cyber actors to traverse Air Force networks, with little intelligence could do to provide actionable data for preemptive defensive actions. Within this cyber defense context, "there will never be enough network defenses to go around" according to Lt Col Vickery.[31] From his perspective, there is great potential for intelligence to guide cyber defense placement and strategy to best protect critical Air Force missions and the associated networks.

This sentiment is shared by Lt Col Paul Williams, commander of the 26th Network Operations Squadron (26 NOS) at Maxwell Air Force Base's Gunter Annex. The 26 NOS is responsible for cyber operations and defense of the Air Force Gateways, which provide connectivity to the Department of Defense Global Information Grid (GIG) and mission critical long haul circuits. The 26 NOS teams with the 33rd Network Warfare Squadron (33 NWS) to operate a series of sensors to execute a Defense-In-Depth cyber defense strategy.[32] Under the

existing construct, there is very limited intelligence support for these operations. The intelligence available to support cyber defense is already heavily tasked but severely limited by lack of manpower and systems resources available for the problem set.[33]

Optimizing Intelligence Processes for Cyber Defense

The traditional Air Force operations focus for cyber defense has tended to be centered on defense of the NIPRNET, with squadrons within the 67th Network Warfare Wing (67 NWW) and 688th Information Operations Wing (688 IOW) conducting many aspect of cyber defense. Operational changes and new cyber defense technology within the last two years are pushing capabilities to ever higher levels. This offers the potential for Cyber ISR to drive new types of cyber defense strategies across the Air Force.

Specific to current Air Force cyber defense activities largely focused on defense of the AFNET (NIPRNET), 67 NWW executes the defense of Air Force missions and operations. Large scale defensive cyber operations occur within the following squadrons which are part of the 26th Network Operations Group (26 NOG): 33 NWS, 26 NOS, 26 OSS, 68 NWS and 352 NWS. The 688 IOW conducts focused cyber defense and rapid technology development through the 92 IOS and 90 IOS, as part of the 318th Information Operations Group (318 IOG). The consensus among the operational cyber leaders that were interviewed for this paper is that there will never be enough cyber defenses to go around. The units specified above support the cyber defense mission and have very minimally manned intelligence support activities to craft unit-level operational defensive strategies. The squadrons are making the most of intelligence personnel associated with each mission set, but the organic assets are not sufficient. The existing manpower and associated resources are inadequate for increased cyber support. For reference, the intelligence flight within the 26 OSS, which supports the entire 67 NWW conducting global

cyber operations, has four funded intelligence billets.[34] As can be seen from this example, the cyber intelligence personnel structure is very under resourced for its global mission.

Outside of existing Air Force cyber intelligence structures, the other services tend to depend heavily on National Security Agency (NSA) for analysis support.[35] Each of the other services has a capability for cyber intelligence, but is not well developed. As a previous operational user of cyber intelligence at Pacific Air Forces and 13th Air Force, Lieutenant Colonel Jonathan Snowden backed up this picture.[36] Although a heavy dependence on NSA for intelligence for cyber defense may appear operationally sound, there is a potential to downplay service mission-specific requirements. Snowden further observed long-range cyber analysis focused on specific adversary intentions and capabilities was the focus of the operational Joint Force Air Component Commander within the Pacific Region.[37]

Air Force intelligence units within AFISRA designated to support the defensive cyber mission should be recognized as existing "Centers of Excellence" which can be built upon as the operational imperative for Cyber ISR continues to grow. These established units focus on conducting Cyber ISR analysis based on near-real-time threats or broad general threats not necessarily specific to the Air Force. There is potentially a limited capability to conduct in-depth and long range analysis of specified cyber threats to Air Force missions and networks.

These activities would also benefit greatly from the increased use of data from Air Force cyber defense sensors, which has tremendous potential ISR value. Thus far this data is untapped due to the highly technical nature of the data, lack of analyst personnel resources, as well as data storage challenges. At this time, data storage is prohibitive due to the vast storage capacity requirements.[38] Furthermore, this data may go far to help fill critical vulnerabilities in the cyber

intelligence cycle previously mentioned. Analysis efforts need to aim for a fully integrated cyber intelligence cycle, so it is no longer incomplete when compared to the air and space domains.[39]

As technology continues to evolve, emphasis should be placed on development of processes to fully integrate data from cyber defense sensors into Air Force analysis activities for near-real-time and long-range cyber intelligence analysis. A sustainable PED structure for Cyber ISR should be developed to best support proactive Air Force Defensive Cyber Operations.[40] Fully developed ISR trend analysis will allow for predictive assessment to proactively posture cyber defensive strategies and operations to blunt adversary activities.

The Air Force NTI program within the 35 IS has great untapped potential to focus even larger defensive cyber operations now and in the future. Increased integration of cyber intelligence into operations planning and execution would potentially increase effectiveness, and develop a critical link between intelligence and cyber operations. Critical data is already available from national-level signals and cyber intelligence databases and reporting. At present, the NTI activity is focused at the 624th Operations Center (624 OC) level. The expansion of support relationships beyond 624 OC to support all cyber defense operations activities within the 67 NWW and 688 IOW would provide excellent operational dividends.

Finally, there is another issue worth addressing to improve short-term analysis. The relationship between the Air Force and cleared defense contractors is mostly beyond the scope of this research project. However, given the Air Force dependencies on key cleared defense contractors for next generation weapons systems, and the high level of adversary exploitation of these companies, there is great potential value in providing tailored cyber intelligence data to cleared defense contractors.[41] A recent Deputy Secretary of Defense proposal to share cyber intelligence data with cleared defense contractors was published in a memo to the services; this

has great potential to better defend future Air Force capabilities and missions as there is an opportunity for cleared defense contractors to tighten cyber defenses based on key intelligence data.[42] The feasibility of this program would be an excellent subject for a future Air War College research paper.

Recommendations

Based on research and analysis of existing and future ISR within the Air Force to support defensive operations within the cyberspace domain, this paper recommends the following actions.

Develop a robust cyberspace ISR PED structure:

The Air Force should develop a robust ISR PED capability devoted to cyberspace. With the untapped ISR potential of data from Air Force cyber defense sensors, plus any future data from dedicated cyber ISR sensors, the potential operational contribution is invaluable. Given the incomplete development of the intelligence cycle to support Air Force cyber defense operations, there are existing frameworks within the Air Force which could be expanded. Requirements discussions are in a very early stage. PED capabilities for Cyber ISR are currently not well developed; normalized PED capabilities would drive more effective cyber intelligence reporting and operations.

Identify Resources:

A more detailed study should be conducted by Air Force experts to determine the suitability and associated additional resources required for NASIC to develop a robust capacity to conduct large scale all-source and long range adversary trend analysis of specified adversary cyber threats to Air Force missions and networks. As the Air Force's service intelligence center for established air and space systems, NASIC is uniquely situated for this cyber role. This

perspective for NASIC was also echoed during the interview with Brigadier General Wooton.[43] The author envisions this would require between one to three new squadrons to effectively perform this mission for the Air Force in the long term.

Focus cyber defense:

Cyber ISR resulting from the first two recommendations will provide the capacity to use ISR as the driver to shift cyber defense operations to focus on the highest priority systems only, where the adversary is forecast to most likely operate. This will result in greater cyber mission assurance for key Air Force capabilities/systems such as the F-22, F-35, remotely piloted aircraft, global mobility, special operations, logistics advanced technology and other weapons systems, as well as space and nuclear missions just to name a few.

Reinforce cyber defense resources:

AFISRA and 24th Air Force intelligence resources associated with the cyber defense mission for the Air Force should be greatly reinforced. As intelligence resources are freed up as the Afghanistan commitment gets smaller, a reallocation of intelligence analysis billets distributed among the associated units should be conducted. To do this effectively, a suitable manpower study should be implemented to determine the correct billet increases and associated certifications and training requirements. As ISR personnel resources are shifted from Afghanistan associated support, a substantial amount of those analysts could be devoted to supporting Air Force cyber defense in the future. As the defense budget will continue to get smaller, these existing intelligence personnel resources could be used to better posture AFISRA and 24 AF units for cyber defense support.

Develop a Cyber Defended Asset List:

As Air Force ISR is evolved over time for better cyber defense of Air Force missions, intelligence can then be used to drive a Cyber Defended Asset List at the enterprise level.[44] Since there are never enough cyber defenses to go around, defense needs to focus on the most important missions. Based on operational inputs and the latest near-real-time and long range trend analysis, the concept of a dynamic cyber defended asset list should be fully developed within Air Force cyber operations.

Conclusion

The adoption of these recommendations will best posture the Air Force to defend its critical missions and networks in the future. As the speed and complexity of adversary capabilities within cyberspace continues to evolve, the Air Force must aggressively defend and preserve the Air Force's qualitative operations advantage, and therefore combat advantage. Furthermore, a more evolved and robust ISR capability for cyber defense can be the impetus to to more fully protect commanders' air, space, and cyber operations.

Notes

1. Matt Egan, *Defense Secretary Panetta Sees a "Pre-9/11 Moment" for Cyber Security,"* Fox Business, 12 October 2012. http://www.foxbusiness.com/government/2012/10/12/ defense-secretary-panetta-sees-pre-11-moment-on-cyber-security/#ixzz2JsYRSyN1 (accessed 13 February 2013).
2. Jeffrey Carr, *Inside Cyber Warfare* (Sebastopol, CA: O'Reilly Media, 2012), 86.
3. Joint Publication 2-1, *Joint Intelligence,* 22 June 2007, I-3.
4. US Air Force Mission Statement, http://www.af.mil/main/welcome.
5. Joint Publication 6-0, Joint Communications System, 10 June 2010, II-2.
6. Brig Gen Kevin B. Wooton., interview with author, 2 November 2012.
7. Joe Keefe. "President's Message." *American Intelligence Journal*, 2011, 2
8. Carr, Ibid, 2.
9. Mark A. Stokes, and L.C. Russell Hsiao, *Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests* (Project 2049, 2012), 2.
10. United States-China Economic and Security Review Commission Report to Congress: "*Chapter 2: China's Cyber Activities,"*(2012), 1.
11. Siobahn Gorman, August Cole, and Yochi Dreazan, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009. http"//www.wsj.com/article/SB124027491029837401.html (accessed 13 February 2013)
12. Carr, *Inside Cyber Warfare*, 217-241.
13. Richard A. Clarke. *Cyber War: The Next Threat To National Security and What To Do About It*. (New York, NY: Harper Collins, 2010), 63.
14. Carr, *Inside Cyber Warfare*, 250-251.
15. Ibid, 4.
16. Ibid, 89-102.
17. Col Carl N. Brenner., interview with author, 29 October 2012.
18. Lt Col Joseph B. Zell., interview with author, 1 November 2012.
19. National Security Agency, "Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments," http://www.nsa.gov/ia/_files/support/defenseindepth.pdf (accessed 13 February 2013)
20. Air Force Doctrine Document (AFDD) 2-0, *Global Integrated Intelligence, Surveillance & Reconnaissance Operations*, 2012, 28.
21. United States Air Force Posture Statement (2012): Statement by General Norton Schwartz (Chief of Staff, United States Air Force) and Mr. Michael B. Donley (Secretary of the Air Force), 2012.
22. Air Force Instruction (AFI) 10-712, *Telecommunications Monitoring And Assessment Program (TMAP)*, 2011, 4.
23. Lt Col Hugh M. Ragland., interview with author, 6 November 2012.
24. Intelligence.gov, "A Dynamic Process Fueling Dynamic Solutions," Office of Director of National Intelligence, http://www.intelligence.gov/about-the-intelligence-community/how-intelligence-works/ (accessed 13 February 2013)
25. Lt Col Scott A. Vickery., interview with author, 6 November 2012.
26. Ibid.
27. Ibid.
28. Ibid.

29. Lt Col Paul D. Williams., interview with author, 16 November 2012.
30. Brett T. Williams, “Ten Propositions Regarding Cyberspace Operations,” *Joint Forces Quarterly* (Issue 61), 13.
31. Lt Col Scott A. Vickery., interview with author, 6 November 2012.
32. Lt Col Paul D. Williams., interview with author, 16 November 2012.
33. Lt Col Scott A. Vickery., interview with author, 6 November 2012.
34. Ibid.
35. Lt Col Jonathan D. Snowden., interview with author, 3 February 2013.
36. Ibid.
37. Ibid.
38. Lt Col Paul D. Williams., interview with author, 16 November 2012.
39. Lt Col Scott A. Vickery., interview with author, 6 November 2012.
40. Lt Col Joseph B. Zell., interview with author, 1 November 2012.
41. Col Timothy D. Haugh., interview with author, 13 November 2012.
42. Ashton B. Carter, Deputy Secretary of Defense to All DoD Agencies and Services, memorandum, 31 October 2012.
43. Brig Gen Kevin B. Wooton., interview with author, 2 November 2012.
44. Lt Col Scott A. Vickery., interview with author, 6 November 2012.

Bibliography

Air Force Doctrine Document (AFDD) 2-0. *Global Integrated Intelligence Surveillance & Reconnaissance Operations*, 6 January 2012.

Air Force Instruction (AFI 10-712), *Telecommunications Monitoring And Assessment Program (TMAP)*, 8 June 2011.

Brenner, Carl N. Col, USAF. NASIC Air & Cyber Analysis Group/CC. Interview by the author. 29 October 2012.

Bush, Frederick E. III, Lt Col, (Author's personal experience).

Carr, Jeffrey. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media, 2012.

Carter, Ashton B, Deputy Secretary of Defense. To All DoD Agencies and Services. Memorandum, 31 October 2012.

Clarke, Richard A. *Cyber War: The Next Threat To National Security and What To Do About It.* New York, NY: Harper Collins, 2010.

Department of the Air Force. *Improving Military Capabilities For Cyber Operations.* Statement by Major General Suzanne M. Vautrinot, Commander, Air Forces Cyber (Twenty-Fourth Air Force). Presentation to the Subcommittee on Emerging Threats and Capabilities, House Armed Services Committee, US House of Representatives, July 2012.

Egan, Matt. *Defense Secretary Panetta Sees a "Pre-9/11 Moment" for Cyber Security."* Fox Business, 12 October 2012. http://www.foxbusiness.com/government/2012/10/12/defense-secretary-panetta-sees-pre-11-moment-on-cyber-security/#ixzz2JsYRSyN1 (accessed 13 February 2013)

Gorman, Siobahn, Cole, August, & Dreazan, Yochi. "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009, http"//www.wsj.com/article/SB124027491029837401.html (accessed 13 February 2013)

Haugh, Timothy D. Col, USAF. 318 IOG/CC. Interview by the author. 13 November 2012.

Intelligence.Gov. "A Dynamic Process Fueling Dynamic Solutions." http://www.intelligence.gov/about-the-intelligence-community/how-intelligence-works/ (accessed 13 February 2013)

Joint Publication 2-1. *Joint Intelligence*, 22 November 2007.

Joint Publication 6-0, *Joint Communications System*, 10 June 2010.

Keefe, Joe. "President's Message." *American Intelligence Journal* Vol. 29, No. 2, 2011: 2.

National Security Agency. “Defense in Depth: A practical strategy for achieving Information Assurance in today’s highly networked environments.” http://www.nsa.gov/ia/_files/support/defenseindepth.pdf (accessed 13 February 2013)

Ragland, Hugh M. III. Lt Col, USAF. 68 NWS/CC. Interview by the author. 6 November 2012.

Snowden, Jonathan D. Lt Col, USAF. Former 13 AF Deputy A2. Interview by the author. 3 February 2013.

Stokes, Mark A., and Hsiao, L.C. Russell. *Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests*. Project 2049, 29 October 2012.

Vickery, Scott A. Lt Col, USAF. 26 OSS/CC. Interview by the author. 6 November 2012.

William, Brett T. “Ten Propositions Regarding Cyberspace Operations,” *Joint Forces Quarterly* (Issue 61), 11-17.

Williams, Paul D. Lt Col, USAF. 26 NOS/CC. Interview by the author. 16 November 2012.

United States Air Force Posture Statement (2012): Statement by General Norton Schwartz (Chief of Staff, United States Air Force) and Mr. Michael B. Donley (Secretary of the Air Force), February 28, 2012.

United States Air Force. “Air Force Mission Statement.” http://www.af.mil/main/welcome.

US Congress. *United States-China Economic and Security Review Commission Report to Congress: Chapter 2: China’s Cyber Activities*, 2012. http://killerapps.foreignpolicy.com/posts/2012/11/14/here_are_the_us_china_commissions_cyber_recommendations (accessed 13 February 2013)

Wooton, Kevin B. Brig Gen, USAF. AFSPC/A6. Interview by the author. 2 November 2012.

Zell, Joseph D. Lt Col, USAF. 33 NWS/CC. Interview by the author. 1 November 2012.